



Galddatora pārvaldības rokasgrāmata

Biznesa galddatori

Dokumenta daļas numurs: 361202-E11

2004. gada maijs

Šajā rokasgrāmatā sniegtas definīcijas un norādījumi par drošības un Intelligent Manageability iespēju lietošanu, kas ir sākotnēji instalētas atsevišķiem modeļiem.

© Autortiesības 2004 Hewlett-Packard Development Company, L.P.
Šajā dokumentā iekļautā informācija var tikt mainīta bez iepriekšēja brīdinājuma.

Microsoft un Windows ir Microsoft Corporation preču zīmes ASV un citās valstīs.

HP produktu un pakalpojumu garantijas ir izklāstītas vienīgi šiem produktiem un pakalpojumiem pievienotajos garantijas paziņojumos. Nekas no šeit minētā nav interpretējams kā papildu garantija. HP neatbild par šajā tekstā pieļautām tehniskām un redakcionālām kļūdām vai izlaidumiem.

Šajā dokumentā ir ietverta patentēta informācija, ko aizsargā autortiesības. Neviena šī dokumenta daļa nedrīkst tikt kopēta, reproducēta vai tulkota kādā citā valodā bez Hewlett-Packard Company iepriekšējas rakstveida piekrišanas.



BRĪDINĀJUMS: Šādi izcelts teksts norāda, ka norādījumu neievērošanas gadījumā ir iespējamās fiziskas traumas vai dzīvības briesmas.



UZMANĪBU! Šādi izcelts teksts norāda, ka norādījumu neievērošanas gadījumā ir iespējams aparātūras bojājums vai informācijas zudums.

Galddatora pārvaldības rokasgrāmata

Biznesa galddatori

Pirmais izdevums (2004. gada maijs)

Dokumenta daļas numurs: 361202-E11

Saturs

Galddatora pārvaldības rokasgrāmata

Sākotnējā konfigurācija un ieviešana	2
Attāla sistēmas instalēšana	3
Programmatūras jaunināšana un pārvaldība	4
Programmatūra HP Client Manager	4
Altiris Client Management Solutions	4
System Software Manager	6
Proactive Change Notification	6
Subscriber's Choice	6
Pārrakstāma ROM	7
Remote ROM Flash	7
HPQFlash	8
FailSafe sāknēšanas bloka ROM	8
Iestatījumu replicēšana	10
Divstāvokļu strāvas poga	18
Globālā tīmekļa vieta	19
„Būvbloki” un partneri	19
Datu izsekošana un drošība	20
Paroles drošība	24
Iestatījumu paroles izveide, izmantojot utilītu Computer Setup	25
Ieslēgšanas paroles izveide, izmantojot utilītu Computer Setup	26
DriveLock	31
Sensors Smart Cover Sensor	32
Slēdzene Smart Cover Lock	34
Master Boot Record Security	36
Pirms pašreizējā sāknēšanas diska nodalīšanas vai formatēšanas	38
Kabeļa slēdzenes nodrošinājums	38
Pirkstu nospiedumu identificēšanas tehnoloģija	39

Kļūdu paziņojumi un atkopšana	39
Disku aizsardzības sistēma	39
Izlīdzinošs barošanas bloks	40
Termiskais sensors	40

Alfabētiskais rādītājs

Galddatora pārvaldības rokasgrāmata

HP pārvaldības risinājums Intelligent Manageability nodrošina standarta risinājumus galddatoru, darbstaciju un piezīmjdatoru pārvaldībai un kontrolei tīkla vidē. 1995. gadā kompānija HP uzsāka datoru pārvaldību, ieviešot nozarē pirmos pilnībā pārvaldāmos galddatorus. HP pieder pārvaldības tehnoloģijas patents. Kopš tā laika kompānija HP šajā nozarē ir ieguldījusi lielu darbu, lai izstrādātu standartus un infrastruktūru, kas nepieciešama efektīvai galddatoru, darbstaciju un piezīmjdatoru ieviešanai, konfigurēšanai un pārvaldībai. HP cieši sadarbojas ar nozares labākajiem pārvaldības programmatūru risinājumu izstrādātājiem, lai nodrošinātu pārvaldības risinājuma Intelligent Manageability un šo produktu saderību. Risinājumam Intelligent Manageability ir nozīmīga loma, īstenojot mūsu vispārējo uzdevumu — nodrošināt lietotājiem datoru risinājumus Lifecycle Solutions, kas tiem palīdzētu četros datora dzīves cikla posmos — plānošanas, ieviešanas, pārvaldības un pārejas posmā.

Galvenās galddatora pārvaldības funkcijas un līdzekļi:

- Sākotnēja konfigurācija un ieviešana
- Attāla sistēmas instalēšana
- Programmatūras jaunināšana un pārvaldība
- Pārrakstāmā ROM
- Datu izsekošana un drošība
- Paziņošana par kļūdām un atkopšana



Atsevišķu šajā rokasgrāmatā aprakstīto līdzekļu atbalsts var atšķirties atkarībā no modeļa vai programmatūras versijas.

Sākotnējā konfigurācija un ieviešana

Dators ir aprīkots ar sākotnēji instalētu sistēmas programmatūras attēlu. Pēc īsa programmatūras „atpakošanas” procesa dators ir gatavs lietošanai.

Iespējams, jūs vēlēsit aizstāt sākotnēji instalēto programmatūras attēlu ar pielāgotu sistēmas un lietojumprogrammu kopu. Pielāgotu programmatūras attēlu var ieviest vairākos veidos:

- pēc sākotnēji instalētās programmatūras attēla atpakošanas, instalējot papildu lietojumprogrammas;
- izmantojot programmatūras ieviešanas rīkus, piemēram, Altiris Deployment Solution™, lai aizstātu sākotnēji instalēto programmatūru ar pielāgotu programmatūras attēlu;
- klonējot diskus, lai viena cietā diska saturu pārkopētu citā cietajā diskā.

Labākā ieviešanas metode ir atkarīga no informāciju tehnoloģiju vides un procesiem. Web vietas HP Lifecycle Solutions sadaļā PC Deployment (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>) ir sniegta informācija par labākajām programmatūras ieviešanas metodēm.

Kompaktdisks *Restore Plus!*, uzstādīšanas no lasāmatmiņas un ACPI aparatūra sniedz palīdzību sistēmas programmatūras atkopšanā, konfigurācijas pārvaldībā, problēmu novēršanā un strāvas pārvaldībā.

Attāla sistēmas instalēšana

Attālās sistēmas instalēšanas līdzeklis ļauj startēt un instalēt sistēmu, izmantojot programmatūru un konfigurācijas informāciju, kas novietota tīkla serverī, inicializējot iespēju Preboot Execution Environment (PXE). Attālās sistēmas instalēšanas līdzeklis parasti tiek izmantots kā sistēmas uzstādīšanas un konfigurēšanas rīks, lai veiktu šādus uzdevumus:

- cietā diska formatēšanu;
- programmatūras attēla ieviešanu vienā vai vairākos datoros;
- attālu sistēmas BIOS jaunināšanu pārrakstāmajā ROM („[Remote ROM Flash](#)” lappusē 7);
- sistēmas BIOS iestatījumu konfigurēšanu.

Lai startētu attālās sistēmas instalēšanas līdzekli, nospiediet taustiņu **F12**, kad ekrānā ar HP logotipu labajā apakšējā stūrī tiek parādīts paziņojums F12 = Network Service Boot (tīkla pakalpojuma sāknēšana). Lai turpinātu darbību, izpildiet ekrānā redzamos norādījumus. Noklusētā sāknēšanas secība ir BIOS konfigurācijas iestatījums, kuru var mainīt, lai iestatītu PXE sāknēšanu.

Kompāniju HP un Altiris sadarbības rezultātā ir izstrādāti rīki, kas atvieglo un paātrina uzņēmumu datoru ieviešanu un pārvaldību, samazinot kopējās izmaksas, tādējādi HP datori ir kļuvuši par vislabāk pārvaldāmajiem klientdatoriem uzņēmumu vidē.

Programmatūras jaunināšana un pārvaldība

HP nodrošina vairākus rīkus galddatoru un darbstaciju programmatūras jaunināšanai un pārvaldībai — programmatūru HP Client Manager, Altiris Client Management Solutions, System Software Manager, Proactive Change Notification un Subscriber's Choice.

Programmatūra HP Client Manager

Programmatūra HP Client Manager (HP CMS) palīdz HP klientiem pārvaldīt viņu klientdatoru aparāturu, izmantojot šādus līdzekļus:

- Detalizētus aparatūras sarakstu skatus datu pārvaldībai;
- Datora darbspēju pārraudzību un diagnostiku;
- Proaktīvu paziņošanu par aparatūras vides izmaiņām;
- No tīkla Web pieejamas uzņēmumam nozīmīgas informācijas paziņošanu, piemēram, ar ierīču pārkaršanu un atmiņas problēmām saistīti brīdinājumi;
- Attālu sistēmas programmatūras, piemēram, ierīču draiveru un BIOS lasāmatmiņas jaunināšanu;
- Attālu sāknēšanas secības maiņu.

Lai iegūtu plašāku informāciju par programmatūru HP Client Manager, apmeklējiet http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Client Management Solutions

Uzņēmumu HP un Altiris sadarbības rezultātā ir tapuši visaptveroši integrēti sistēmu pārvaldības risinājumi, kas palīdz samazināt HP klientdatoru izmaksas. Kopā ar programmatūru HP Client Manager var izmantot papildu risinājumus Altiris Client Management Solutions, kas ietver:

- Inventāra un datu pārvaldību:
 - ❑ programmatūras licences atbilstību;
 - ❑ datoru izsekošanu un ziņošanu;
 - ❑ nomas līgumu, kurā noteikta datu izsekošana.

- Ieviešanu un migrēšanu:
 - ❑ Microsoft Windows XP Professional vai Home Edition migrēšanu;
 - ❑ sistēmas ieviešanu;
 - ❑ lietotāju migrēšanu.
- Palīdzības dienestu un problēmu risināšanu:
 - ❑ palīdzības dienesta paziņojumu pārvaldību;
 - ❑ attālu problēmu novēršanu;
 - ❑ attālu problēmu risināšanu;
 - ❑ klientdatoru kļūmju atkopšanu.
- Programmatūras un darbību pārvaldību:
 - ❑ nepārtrauktu galddatoru pārvaldību;
 - ❑ HP sistēmas programmatūras ieviešanu;
 - ❑ lietojumprogrammu pašatjaunošanos.

Plašāku informāciju un norādījumus, kā lejupielādēt pilnas funkcionalitātes Altiris risinājumu 30 dienu iepazīšanās versiju, varat iegūt <http://h18000.www1.hp.com/im/prodinfo.html#deploy>.

Atsevišķiem galddatoru un piezīmjdatoru modeļiem kā daļa no rūpnīcā ielādētā attēla ir iekļauts Altiris pārvaldības aģents. Šis aģents nodrošina sakarus ar risinājumu Altiris Development Solution, kurš ļauj veikt aparatūras ieviešanu vai lietotāju migrēšanu uz jaunu operētājsistēmu, izmantojot vienkārši lietojamus vedņus. Altiris risinājumi piedāvā viegli lietojamas programmatūras izvietšanas iespējas. Lietojot tās kopā ar utilītu System Software Manager vai programmatūru HP Client Manager, administratori var arī jaunināt BIOS lasāmatmiņu un ierīču draiveru programmatūru no galvenās pults.

Lai iegūtu plašāku informāciju, apmeklējiet <http://h18000.www1.hp.com/im/index.html>.

System Software Manager

System Software Manager (SSM) ir utilīta, kas ļauj jaunināt sistēmas programmatūru vienlaicīgi vairākās sistēmās. Veicot klientdatoru sistēmas jaunināšanu, SSM nosaka gan aparatūras, gan programmatūras versiju, pēc tam jaunina atbilstošo programmatūru no centrālā repozitorija, kas tiek saukts arī par failu krātuvi. SSM atbalstītās draiveru versijas ir norādītas ar īpašu ikonu draiveru lejupielādes Web vietā un atbalsta programmatūras kompaktdiskā Support Software. Lai lejupielādētu šo utilītu vai iegūtu plašāku informāciju par SSM, apmeklējiet <http://www.hp.com/go/ssm>.

Proactive Change Notification

Programma Proactive Change Notification lieto Web vietu Subscriber's Choice, lai proaktīvi un automātiski:

- nosūtītu Proactive Change Notification (PCN) e-pasta ziņojumu par aparatūras un programmatūras izmaiņām lielākajai daļai komerciālo datoru un serveru līdz pat 60 dienām iepriekš;
- nosūtītu e-pasta ziņojumu, kurā ietverti informatīvie materiāli Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins un ar draiveru problēmām saistīti brīdinājumi lielākajai daļai komerciālo datoru un serveru.

Izveidojiet pielāgotu profilu, lai nodrošinātu tikai noteiktai IT videi atbilstošas informācijas saņemšanu. Lai iegūtu plašāku informāciju par programmu Proactive Change Notification un izveidotu pielāgotu profilu, apmeklējiet <http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn>.

Subscriber's Choice

Subscriber's Choice ir klientiem paredzēts HP pakalpojums. Atbilstoši lietotāja izveidotajam profilam HP nosūta individuālus padomus par produktiem, informāciju par līdzekļiem un/vai draiveru un atbalsta brīdinājumus/paziņojumus. Izmantojot Subscriber's Choice Driver un Support Alerts/Notifications, tiek nosūtīti e-pasta ziņojumi, lai informētu par iespēju pārskatīt un izgūt savā profilā abonēto informāciju. Lai uzzinātu vairāk par pakalpojumu Subscriber's Choice un izveidotu pielāgotu profilu, apmeklējiet <http://h30046.www3.hp.com/subhub.php>.

Pārrakstāma ROM

Datora komplektācijā iekļauta programmējama pārrakstāma ROM. Norādot iestatījumu paroli, izmantojot utilītu Computer Setup (F10), lasāmatmiņu var aizsargāt pret netīšu jaunināšanu vai pārrakstīšanu. Tā ir nepieciešama, lai nodrošinātu datora darbības integritāti. Ja vēlaties jaunināt lasāmatmiņu, varat:

- pasūtīt HP jauninātu ROMPaq disketi;
- lejupielādēt jaunākos ROMPaq attēlus no HP draiveru un atbalsta lapas: <http://www.hp.com/support/files>.



UZMANĪBU! Lai gūtu maksimālu ROM aizsardzību, norādiet iestatījumu paroli. Iestatījumu parole novērš nesankcionētu ROM jaunināšanu. Utilīta System Software Manager ļauj sistēmas administratoram iestatīt iestatījumu paroli vienā vai vairākos datoros vienlaicīgi. Lai iegūtu plašāku informāciju, apmeklējiet <http://www.hp.com/go/ssm>.

Remote ROM Flash

Utilīta Remote ROM Flash ļauj sistēmas administratoram droši jaunināt attālu HP datoru lasāmatmiņu tieši no centralizētās tīkla vadības pults. Tā kā sistēmas administrators var veikt šo uzdevumu attāli vairākos datoros un personīgajos datoros, tīklā pastāvīgi tiek veikta HP datoru ROM attēlu ieviešana, un tos var efektīvāk pārvaldīt. Šādi tiek panākta arī augstāka produktivitāte un samazinātas kopējās izmaksas.



Lai izmantotu priekšrocības, datoram jābūt pieslēgtam pie strāvas un ieslēgtam, izmantojot Remote Wakeup.

Plašāku informāciju par s skatiet sadaļā HP Client Manager Software vai System Software Manager, apmeklējot <http://h18000.www1.hp.com/im/prodinfo.html>.

HPQFlash

Utilīta HPQFlash tiek lietota, lai lokāli jauninātu vai atjaunotu atsevišķu datoru sistēmas lasāmatmiņu, izmantojot operētājsistēmu Windows.

Lai iegūtu plašāku informāciju par utilītu HPQFlash, apmeklējiet <http://www.hp.com/support/files> un pēc uzaicinājuma ievadiet datora nosaukumu.

FailSafe sāknēšanas bloka ROM

FailSafe sāknēšanas bloka ROM ļauj atkopt sistēmu pārrakstāmās ROM kļūmes gadījumā (maz iespējams), piemēram, ja ROM jaunināšanas laikā tiek pārtraukta strāvas padeve. Sāknēšanas bloks ir pret pārrakstīšanu aizsargāta lasāmatmiņas daļa, kas meklē derīgu pārrakstāmu sistēmas ROM, kad sistēmai ir pieslēgta strāva.

- Ja sistēmas ROM ir derīga, sistēma tiek startēta kā parasti.
- Ja sistēmas ROM neatbilst derīguma pārbaudes prasībām, FailSafe sāknēšanas bloka ROM atbalsta sistēmas startēšanu no ROMPaq disketes, kas programmē sistēmas ROM ar derīgu attēlu.



Daži modeļi nodrošina arī atkopšanu no kompaktdiska ROMPaq. ISO ROMPaq attēli ir iekļauti atsevišķiem modeļiem lejupielādējamās programmatūras komplektā ROM.

Kad sāknēšanas bloks atklāj nederīgu sistēmas ROM, sistēmas strāvas indikators mirgo 8 reizes (vienreiz sekundē), pēc tam ieturot 2 sekunžu pauzi. Ir dzirdami arī 8 sinhroni pīkstieni. Ekrānā tiek parādīts sāknēšanas bloka atkopšanas režīma paziņojums (dažiem modeļiem).

Lai atkoptu sistēmu pēc tās ieviešanas sāknēšanas bloka atkopšanas režīmā, izpildiet šos soļus:

1. Ja diskešu vai kompaktdisku diskdzinī ir attiecīgi diskete vai kompaktdisks, izņemiet tos un pārtrauciet strāvas padevi.
2. Ievietojiet ROMPaq disketi diskešu diskdzinī vai, ja šim datoram ir atļauts, ROMPaq kompaktdisku tam paredzētajā diskdzinī.

3. Ieslēdziet datoru.

Ja dators neatrod ROMPaq disketi vai ROMPaq kompaktdisku, tiek parādīts uzaicinājums ievietot kādu no tiem un restartēt datoru.

Ja ir izveidota iestatījumu parole, tiek iedegts indikators Caps Lock un parādīts uzaicinājums ievadīt paroli.

4. Ievadiet iestatījumu paroli.

Ja sistēma tiek veiksmīgi startēta no disketes un ROM tiek pārprogrammēta, tiek iedegti visi trīs tastatūras indikatori. Par veiksmīgu darbību izpildi norāda arī kāpjošu signālu secība.

5. Izņemiet disketi vai kompaktdisku un izslēdziet datoru.

6. Ieslēdziet datoru no jauna, lai to restartētu.

Šajā tabulā norādītas dažādas tastatūras indikatoru kombinācijas, ko izmanto sāknēšanas bloka ROM (ja datoram ir pievienota PS/2 tastatūra), kā arī sniegti paskaidrojumi par katras kombinācijas nozīmi un darbību.

Sāknēšanas bloka ROM lietotās tastatūras indikatoru kombinācijas

Režims FailSafe Boot Block	Tastatūras indikatora krāsa	Tastatūras indikatora darbība	Stāvoklis/paziņojums
Num Lock	Zaļa	Iedegts	ROMPaq diskete vai ROMPaq kompaktdisks nav ievietots, ir bojāts vai diskdzinis nav gatavs darbam.
Caps Lock	Zaļa	Iedegts	Ievadiet paroli.
Num, Caps, Scroll Lock	Zaļa	Mirgo pēc kārtas – N, C, SL	Tastatūra ir slēgta tīkla režīmā.
Num, Caps, Scroll Lock	Zaļa	Iedegti	Sāknēšanas bloka ROM ir sekmīgi pārrakstīta. Izslēdziet datoru, pēc tam ieslēdziet, lai veiktu atkārtotu sāknēšanu.



USB tastatūru diagnostikas indikatori nemirgo.

Iestatījumu replicēšana

Ar šo procedūru administrators var viegli iekopēt datora iestatījumu konfigurāciju citos tāda paša modeļa datoros. Šādi var ātrāk un saskaņotāk veikt vairāku datoru konfigurāciju.



Lai veiktu abas šīs darbības, ir nepieciešams diskešu diskdzinis vai atbalsfīts USB zibatmiņas datu nesējs, piemēram, atslēga HP Drive Key.

Kopēšana vienā datorā



UZMANĪBU! Iestatījumu konfigurācija ir atkarīga no datora modeļa. Ja datora, no kura tiek veikta kopēšana, modelis nav vienāds ar tā datora modeli, kurā jākopē, var rasties failu sistēmas bojājums. Piemēram, nekopējiet galddatora dc7100 Ultra-Slim Desktop iestatījumu konfigurāciju datorā dx6100 Slim Tower.

1. Izvēlieties iestatījumu konfigurāciju, kura jākopē. Izslēdziet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Shut Down (Beidzēšana)**.
 2. Ja lietojat USB zibatmiņas datu nesēju, ievietojiet to.
 3. Ieslēdziet datoru.
 4. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.
-



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Ja, lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

5. Ja lietojat disketi, ievietojiet to.
6. Noklikšķiniet uz **File > Replicated Setup > Save to Removable Media**. Lai izveidotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju, izpildiet ekrānā redzamos norādījumus.
7. Izslēdziet datoru, kuru vēlaties konfigurēt, un ievietojiet konfigurēšanas disketi vai USB zibatmiņas datu nesēju.

8. Ieslēdziet datoru, kurš jākonfigurē.
9. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.
10. Noklikšķiniet uz **File > Replicated Setup > Restore from Removable Media** un izpildiet ekrānā redzamos norādījumus.
11. Kad konfigurēšana ir pabeigta, restartējiet datoru.

Kopēšana vairākos datoros



UZMANĪBU! Iestatījumu konfigurācija ir atkarīga no datora modeļa. Ja datora, no kura tiek veikta kopēšana, modelis nav vienāds ar tā datora modeli, kurā jākopē, var rasties faila sistēmas bojājums. Piemēram, nekopējiet galddatora dc7100 Ultra-Slim Desktop iestatījumu konfigurāciju datorā dx6100 Slim Tower.

Lai sagatavotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju atbilstoši šai metodei, nepieciešams daudz vairāk laika, taču konfigurācija tiek iekopēta mērķdatoros ievērojami ātrāk.



Lai veiktu šo procedūru, ir nepieciešama sāknēšanas diskete vai izveidots USB zibatmiņas datu nesējs, ar kuru var veikt sāknēšanu. Ja sāknēšanas disketes izveidošanai nav pieejama operētājsistēma Windows XP, veiciet darbības, kas paredzētas kopēšanai vienā datorā (sk. „[Kopēšana vienā datorā](#)” lappusē 10).

1. Izveidojiet sāknēšanas disketi vai USB zibatmiņas datu nesēju. Sk. „[Atbalstīts USB zibatmiņas datu nesējs](#)” lappusē 13, vai „[Neatbalstīts USB zibatmiņas datu nesējs](#)” lappusē 16.



UZMANĪBU! Visus datorus nevar sāknēt no USB pārrakstāmā datu nesēja. Ja utilītas Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB datu nesējs ir norādīts pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diskete.

2. Izvēlieties iestatījumu konfigurāciju, kas jākopē. Izslēdziet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Shut Down (Beidzēšana)**.

3. Ja lietojat USB zibatmiņas datu nesēju, ievietojiet to.
4. Ieslēdziet datoru.
5. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Ja, lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

6. Ja lietojat disketi, ievietojiet to.
7. Noklikšķiniet uz **File > Replicated Setup > Save to Removable Media**. Lai izveidotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju, izpildiet ekrānā redzamos norādījumus.
8. Lai replicētu iestatījumus, lejupielādējiet utilītu BIOS (repset.exe) un iekopējiet to konfigurēšanas disketē vai USB zibatmiņas datu nesējā. Lai iegūtu šo utilītu, dodieties uz <http://welcome.hp.com/support/files> un ievadiet datora modeļa numuru.
9. Konfigurēšanas disketē vai USB zibatmiņas datu nesējā izveidojiet failu autoexec.bat, kas ietver šādu komandu:
repset.exe
10. Izslēdziet konfigurējamo datoru. Ievietojiet konfigurēšanas disketi vai USB zibatmiņas datu nesēju un ieslēdziet datoru. Automātiski tiek palaista konfigurēšanas utilīta.
11. Kad konfigurēšana ir pabeigta, restartējiet datoru.

Sāknēšanas ierīces izveide

Atbalstīts USB zibatmiņas datu nesējs

Atbalstītajām ierīcēm, piemēram, atslēgai HP Drive Key vai DiskOnKey, ir sākotnēji instalēts attēls, lai atvieglotu to pārveidi par sāknēšanas ierīcēm. Ja izmantotajam USB zibatmiņas datu nesējam nav šī attēla, veiciet šajā nodaļā tālāk norādītās darbības (sk. „[Atbalstīts USB zibatmiņas datu nesējs](#)” lappusē 16).



UZMANĪBU! Visus datorus nevar sāknēt no USB zibatmiņas datu nesēja. Ja utilitās Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce ir norādīta pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diske.

Lai izveidotu USB zibatmiņas datu nesēju, ar kuru var veikt sāknēšanu, jums jāiegādājas:

■ Kāda no šīm sistēmām:

- ☐ HP Compaq dc7100 sērijas biznesa galddators;
- ☐ HP Compaq dx6100 sērijas biznesa galddators;
- ☐ HP Compaq d530 sērijas biznesa galddators — Ultra-Slim Desktop, Small Form Factor vai Convertible Minitower;
- ☐ Compaq Evo D510 Ultra-slim Desktop;
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor.

Atkarībā no konkrētā BIOS nākamās sistēmas, iespējams, atbalstīs sāknēšanu uz USB zibatmiņas datu nesēju.



UZMANĪBU! Ja lietojat datoru, kas nav minēts šajā sarakstā, pārliedzinieties, vai utilitās Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce norādīta pirms cietā diska.

■ Kāds no šiem atmiņas moduļiem:

- ☐ 16 MB HP Drive Key;
- ☐ 32 MB HP Drive Key;
- ☐ 32 MB DiskOnKey;
- ☐ 64 MB HP Drive Key;

- ☐ 64 MB DiskOnKey;
 - ☐ 128 MB HP Drive Key;
 - ☐ 128 MB DiskOnKey;
 - ☐ 256 MB HP Drive Key;
 - ☐ 256 MB DiskOnKey.
- DOS diskete, ar kuru var veikt sāknēšanu un kurā iekļautas programmas FDISK un SYS. Ja programma SYS nav pieejama, var lietot programmu FORMAT, taču tādā gadījumā tiks zaudēti visi USB zibatmiņas datu nesējā esošie faili.
1. Izslēdziet datoru.
 2. Ievietojiet USB zibatmiņas datu nesēju kādā no datora USB portiem un noņemiet visas pārējās USB atmiņas ierīces, izņemot USB diskešu diskdziņus.
 3. Ievietojiet diskešu diskdziņā DOS disketi, ar kuru var veikt sāknēšanu un kurā ietvertas programmas FDISK.COM un SYS.COM vai FORMAT.COM, pēc tam ieslēdziet datoru, lai veiktu sāknēšanu uz DOS disketi.
 4. Palaidiet programmu FDISK no uzvednes A:\, ievadot **FDISK** un nospiežot taustiņu Enter. Ja tiek parādīts uzaicinājums, noklikšķiniet uz **Yes (Y)**, lai aktivizētu ietilpīgu disku atbalstu.
 5. Ievadiet Choice [**5**], lai parādītu sistēmā esošos diskdziņus. USB zibatmiņas datu nesējs būs tas diskdziņis, kura lielums līdzinās kādam no sarakstā norādītajiem diskdziņiem. Parasti tas ir pēdējais saraksta diskdziņis. Pierakstiet diskdziņa burtu.
USB zibatmiņas datu nesēja diskdziņis: _____



UZMANĪBU! Ja diskdziņis neatbilst USB zibatmiņas datu nesējam, neturpiniet darbības. Pretējā gadījumā varat zaudēt datus. Pārbaudiet, vai kādā no USB portiem nav papildu atmiņas ierīce. Ja atrodiat atmiņas ierīces, noņemiet tās, vēlreiz sāknējiet datoru un turpiniet darbības no 4. soļa. Ja ierīces netiek atrastas, iespējams, sistēma neatbalsta USB zibatmiņas datu nesēju vai USB zibatmiņas datu nesējs ir bojāts. **NETURPINIET** USB zibatmiņas datu nesēja pārveidošanu par sāknēšanas ierīci.

6. Izejiet no programmas FDISK, nospiežot taustiņu **Esc**, tādējādi atgriežoties uzvednē A:\.

7. Ja DOS sāknēšanas disketē ietverta programma SYS.COM, pārejiet uz 8. soli. Pretējā gadījumā pārejiet uz 9. soli.
8. Uzvednē A:\ ievadiet **SYS x:**, x vietā norādot iepriekš pierakstīto burtu.



UZMANĪBU! Ievadiet USB zibatmiņas datu nesējam atbilstošo diska burtu.

Kad sistēmas faili ir pārsūtīti, programma SYS atgriežas uzvednē A:\. Pārejiet uz 13. soli.

9. USB zibatmiņas datu nesēja failus, kurus vēlaties paturēt, iekopējiet cita diska (piemēram, sistēmas iekšējā cietā diska) pagaidu direktorijā.
10. Uzvednē A:\ ievadiet **FORMAT /S X:**, X vietā norādot iepriekš pierakstīto burtu.



UZMANĪBU! Ievadiet USB zibatmiņas datu nesējam atbilstošo diska burtu.

Programma FORMAT parāda vienu vai vairākus brīdinājumus un ikreiz vaicā, vai vēlaties turpināt. Katru reizi ievadiet **Y**. Programma FORMAT veic USB zibatmiņas datu nesēja formatēšanu, pievieno sistēmas failus un prasa norādīt sējuma etiķeti.

11. Nospiediet taustiņu **Enter**, ja nevēlaties ievadīt etiķeti, vai ievadiet to, ja vēlaties.
12. Kopējiet 9. solī saglabātos failus atpakaļ USB zibatmiņas datu nesējā.
13. Izņemiet disketi un no jauna sāknējiet datoru. Dators veiks sāknēšanu uz USB zibatmiņas datu nesēju kā uz C disku.



Noklusētā sāknēšanas secība dažādiem datoriem atšķiras, un to var mainīt, izmantojot utilītu Computer Setup (F10).

Ja izmantojāt Windows 9x DOS versiju, tiek parādīts ekrāns ar Windows logotipu. Ja nevēlaties, lai šis ekrāns tiktu rādīts, USB zibatmiņas datu nesēja saknes direktorijam pievienojiet nulles lieluma failu LOGO.SYS.

Atgriezieties sadaļā „[Kopēšana vairākos datoros](#)” lappusē 11.

Neatbalstīts USB zibatmiņas datu nesējs



UZMANĪBU! Visus datorus nevar sāknēt no USB zibatmiņas datu nesēja. Ja utilitās Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce ir norādīta pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diskete.

Lai izveidotu sāknēšanas USB zibatmiņas datu nesēju, jābūt:

■ Kādam no šīm sistēmām:

- ☐ HP Compaq dc7100 sērijas biznesa galddators
- ☐ HP Compaq dx6100 sērijas biznesa galddators
- ☐ HP Compaq d530 sērijas biznesa galddators — Ultra-Slim Desktop, Small Form Factor vai Convertible Minitower
- ☐ Compaq Evo D510 Ultra-slim Desktop
- ☐ Compaq Evo D510 Convertible Minitower/Small Form Factor

Atkarībā no konkrētā BIOS nākamās sistēmas, iespējams, atbalstīs sāknēšanu uz USB zibatmiņas datu nesēju.



UZMANĪBU! Ja lietojat datoru, kas nav minēts šajā sarakstā, pārliecinieties, vai utilitās Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce norādīta pirms cietā diska.

■ DOS sāknēšanas disketei, kurā iekļautas programmas FDISK un SYS. Ja programma SYS nav pieejama, var lietot programmu FORMAT, taču tādā gadījumā tiks zaudēti visi USB zibatmiņas datu nesēja faili.

1. Ja sistēmā ir PCI kartes, kurām pievienoti SCSI, ATA RAID vai SATA diskdziņi, izslēdziet datoru un atvienojiet strāvas vadu.



UZMANĪBU! Strāvas vadam JĀBŪT atvienotam.

2. Noņemiet datora pārsegu un izņemiet PCI kartes.
3. Ievietojiet USB zibatmiņas datu nesēju kādā no datora USB portiem un noņemiet visas pārējās USB atmiņas ierīces, izņemot USB diskešu diskdziņus. Uzlieciet datora pārsegu.

4. Pievienojiet strāvas vadu un ieslēdziet datoru.
5. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Ja, lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

6. Dodieties uz **Advanced > PCI Devices**, lai deaktivizētu gan PATA gan SATA kontrollerus. Atspējojot SATA kontrolleri, pierakstiet pieprasījumu IRQ, kuram šis kontrolleris ir piesaistīts. Vēlāk pieprasījums IRQ būs jāpiesaista no jauna. Izejiet no iestatījumiem, apstiprinot izmaiņas.
SATA pieprasījumu IRQ: _____
7. Ievietojiet diskešu diskdziņī sāknēšanas DOS disketi, kurā ietvertas programmas FDISK.COM un SYS.COM vai FORMAT.COM, pēc tam ieslēdziet datoru, lai veiktu sāknēšanu uz DOS disketi.
8. Palaidiet programmu FDISK un izdzēsiet esošos USB zibatmiņas datu nesēja nodalījumus. Izveidojiet jaunu nodalījumu un atzīmējiet to kā aktīvu. Izejiet no programmas FDISK, nospiežot taustiņu **Esc**.
9. Ja, izejot no programmas FDISK, sistēma netika automātiski restartēta, nospiediet taustiņu kombināciju **Ctrl+Alt+Del**, lai no jauna veiktu sāknēšanu uz DOS disketi.
10. Uzvednē A:\ ievadiet **FORMAT C: /S** un nospiediet taustiņu **Enter**. Programma Format veic USB zibatmiņas datu nesēja formatēšanu, pievieno sistēmas failus un prasa norādīt sējuma etiķeti.
11. Nospiediet taustiņu **Enter**, ja nevēlaties ievadīt etiķeti, vai ievadiet to, ja vēlaties.
12. Izslēdziet datoru un atvienojiet strāvas vadu. Atveriet datora pārsegu un no jauna uzstādiat noņemtās PCI kartes. Uzlieciet datora pārsegu.
13. Pievienojiet strāvas vadu, izņemiet disketi un ieslēdziet datoru.

14. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.
15. Dodieties uz **Advanced > PCI Devices** un no jauna aktivizējiet PATA un SATA kontrollerus, kuri 6. solī tika deaktivizēti. Novietojiet SATA kontrolleri atbilstoši tā sākotnējam pieprasījumam IRQ.
16. Saglabājiet izmaiņas un izejiet no programmas. Dators veic sāknēšanu uz USB zibatmiņas datu nesēju kā uz C disku.



Noklusētā sāknēšanas secība dažādiem datoriem atšķiras, un to var mainīt, izmantojot utilītu Computer Setup (F10). Norādījumus skatiet *dokumentācijas kompaktdiskā* ietvertajā *Computer Setup rokasgrāmatā*.

Ja izmantojāt Windows 9x DOS versiju, tiek parādīts ekrāns ar Windows logotipu. Ja nevēlaties, lai šis ekrāns tiktu rādīts, USB zibatmiņas datu nesēja saknes direktorijam pievienojiet nulles lieluma failu LOGO.SYS.

Atgriezieties sadaļā „[Kopēšana vairākos datoros](#)” lappusē 11.

Divstāvokļu strāvas poga

Ja ir aktivizēts interfeiss Advanced Configuration and Power Interface (ACPI), strāvas pogu var lietot gan kā ieslēgšanas/izslēgšanas slēdzi, gan kā gaidstāves pogu. Izmantojot gaidstāvi, dators pilnībā netiek izslēgts, bet tiek darbināts gaidstāves režīmā ar minimālu strāvas padevi. Šādi var ātri pazemināt strāvas padevi, neizejot no lietojumprogrammām, un atgriezties iepriekšējā darba režīmā, nezaudējot datus.

Lai mainītu strāvas pogas konfigurāciju, veiciet šādas darbības:

1. Ar peles kreiso taustiņu noklikšķiniet uz **Start Button**, pēc tam izvēlieties **Control Panel > Power Options**.
2. Logā **Power Options Properties**, izvēlieties zīmni **Advanced**.
3. Sadaļā **Power Button** izvēlieties **Stand by**.

Kad strāvas pogu esat konfigurējis darbībai gaidstāves režīmā, nospiediet strāvas pogu, lai sistēma darbotos minimālas strāvas padeves režīmā (gaidstāvē). Nospiediet pogu vēlreiz, lai sistēma ātri atgrieztos pilnas jaudas režīmā. Lai sistēmai pilnībā atslēgtu strāvas padevi, nospiediet un turiet strāvas pogu četras sekundes.



UZMANĪBU! Nelietojiet strāvas pogu, lai izslēgtu datoru, ja sistēma reaģē; strāvas izslēgšana, neizmantojot operētājsistēmu, var bojāt cieto disku vai izraisīt datu zudumu.

Globālā tīmekļa vieta

HP inženieri rūpīgi pārbauda un atklūdo HP un trešo pušu piegādātāju izstrādāto programmatūru, kā arī izstrādā operētājsistēmas atbalsta programmatūru, lai nodrošinātu HP datoru veikspēju, saderību un uzticamību.

Pārejot uz jaunu vai mainītu operētājsistēmu, ir svarīgi lietot attiecīgajai operētājsistēmai izstrādātu atbalsta programmatūru. Ja plānojat palaist Microsoft Windows versiju, kas atšķiras no datorā iekļautās versijas, jāinstalē atbilstoši ierīču draiveri un utilītas, lai nodrošinātu visu līdzekļu atbalstu un pareizu darbību.

HP ir atvieglājusi jaunākās atbalsta programmatūras atrašanu, piekļuvi tai, kā arī tās novērtēšanu un instalēšanu. Programmatūru var lejupielādēt no Web vietas <http://www.hp.com/support>.

Šajā Web vietā iekļauti jaunākie ierīču draiveri, utilītas un pārrakstāmās ROM attēli, kas nepieciešami, lai HP datoros palaistu jaunāko operētājsistēmu Microsoft Windows.

„Būvbloki” un partneri

HP pārvaldības risinājumi ir saskaņoti ar citām sistēmu pārvaldības lietojumprogrammām un atbilst šādiem nozares standartiem:

- Web-Based Enterprise Management (WBEM);
- Windows Management Interface (WMI);
- Tehnoloģija Wake on LAN;
- Interfeiss ACPI;
- SMBIOS;
- Pre-boot Execution (PXE) atbalsts.

Datu izsekošana un drošība

Datorā iekļautais datu izsekošanas līdzeklis nodrošina galvenos izsekošanas datus, ko var pārvaldīt, izmantojot programmu HP Systems Insight Manager, HP Client Manager vai citu sistēmas pārvaldības lietojumprogrammu. Vienlaidu automātiskā datu izsekošanas līdzekļa un šo produktu integrācija ļauj izvēlēties pārvaldības rīku, kas vislabāk atbilst konkrētajai videi, un racionāli ieguldīt līdzekļus esošajos rīkos.

HP piedāvā arī vairākus risinājumus, kas ļauj vadīt piekļuvi vērtīgiem komponentiem un informācijai. Ja ir instalēts līdzeklis ProtectTools Embedded Security, tas novērš nesankcionētu piekļuvi datiem, kā arī pārbauda sistēmas integritāti un autentificē trešās puses lietotājus, kuri mēģina piekļūt sistēmai (plašāku informāciju skatiet *dokumentācijas kompaktdiska sadaļā Darba sākšana, HP ProtectTools Embedded Security Manager*). Drošības līdzekļi ProtectTools, sensors Smart Cover Sensor un slēdzene Smart Cover Lock, kas pieejami atsevišķiem modeļiem, novērš nesankcionētu piekļuvi datora iekšējiem komponentiem. Deaktivizējot paralēlos, seriālos vai USB portus vai deaktivizējot noņemamo datu nesēju sāknēšanas iespēju, var aizsargāt vērtīgus datus. Memory Change un sensora Smart Cover Sensor brīdinājumus var automātiski pārsūtīt uz sistēmas pārvaldības lietojumprogrammām, lai tiktu nosūtīti proaktīvi paziņojumi par datora iekšējo komponentu mainīšanu.






Līdzekļi ProtectTools, sensors Smart Cover Sensor un slēdzene Smart Cover Lock ir iespējas, kas pieejamas atsevišķām sistēmām.

Lai pārvadītu HP datora drošības iestatījumus, lietojiet šādas utilītas:


- Lokāli lietojiet utilītu Computer Setup. Plašāku informāciju un norādījumus par utilītas Computer Setup lietošanu skatiet *dokumentācijas kompaktdiskā iekļautajā Utilītas Computer Setup (F10) rokasgrāmātā*.
- Attāli lietojiet programmatūru HP Client Manager vai System Software Manager. Šī programmatūra nodrošina drošības iestatījumu drošu, saskaņotu ieviešanu un vadību no vienkāršas komandrindas utilītas.

Šajā tabulā un sadaļās sniegta informācija par datora drošības līdzekļu lokālo vadīšanu, izmantojot utilītu Computer Setup (F10).




Drošības līdzekļu pārskats

Iespēja	Apraksts
Setup Password	<p>Ļauj iestatīt un aktivizēt iestatījumu (administratora) paroli.</p> <p> Ja ir iestatīta iestatījumu parole, ir nepieciešams mainīt Computer Setup iespējas, pārrakstīt ROM un mainīt atsevišķus Windows standarta Plug and Play iestatījumus.</p> <p>Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Problēmu novēršanas rokasgrāmātā</i>.</p>
Power-On Password	<p>Ļauj iestatīt un aktivizēt ieslēgšanas paroli.</p> <p>Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Problēmu novēršanas rokasgrāmātā</i>.</p>
Password Options (šī iespēja tiek parādīta tikai tad, ja ieslēgšanas parole ir iestatīta.)	<p>Ļauj norādīt, vai siltajai sāknēšanai ir nepieciešama parole (CTRL+ALT+DEL).</p> <p>Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Galddatora pārvaldības rokasgrāmātā</i>.</p>
Pre-Boot Authorization	<p>Ļauj aktivizēt/deaktivizēt viedkarti, kas lietojama ieslēgšanas paroles vietā.</p>
Smart Cover	<p>Ļauj:</p> <ul style="list-style-type: none"> Aktivizēt/deaktivizēt slēdzeni Cover Lock. Aktivizēt/deaktivizēt sensoru Cover Removal Sensor. <p> <i>Notify User</i> brīdina lietotāju, ka sensors ir noteicis pārsega noņemšanu. Iespēja Setup Password pieprasa ievadīt iestatījumu paroli, lai sāknētu datoru, ja sensors ir noteicis pārsega noņemšanu.</p> <p>Šis līdzeklis tiek atbalstīts tikai atsevišķiem modeļiem. Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Galddatora pārvaldības rokasgrāmātā</i>.</p>
<p> Plašāku informāciju par utilītu Computer Setup skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Utilītas Computer Setup (F10) rokasgrāmātā</i>.</p> <p>Drošības līdzekļu atbalsts var atšķirties atkarībā no konkrētās datora konfigurācijas.</p>	




Drošības līdzekļu pārskats (turpinājums)

Iespēja	Apraksts
Embedded Security	<p>Ļauj:</p> <ul style="list-style-type: none"> Aktivizēt/deaktivizēt iegulto drošības ierīci. Ierīcei atjaunot rūpnīcas iestatījumus. <p>Šis līdzeklis tiek atbalstīts tikai atsevišķiem modeļiem. Plašāku informāciju skatiet <i>dokumentācijas kompaktdiska</i> dokumentā <i>HP ProtectTools Embedded Security Guide</i>.</p>
Device Security	<p>Aktivizē/deaktivizē seriālos un paralēlos portus, priekšējos USB portus, sistēmas audioirīces, tīkla kontrollerus (atsevišķiem modeļiem), MultiBay ierīces (atsevišķiem modeļiem) un SCSI kontrollerus (atsevišķiem modeļiem).</p>
Network Service Boot	<p>Aktivizē/deaktivizē datora spēju veikt sāknēšanu no tīkla serverī instalētas operētājsistēmas (šis līdzeklis pieejams tikai NIC modeļiem; tīkla kontrollerim jāatrodas kopnē PCI vai jābūt iegultam sistēmas platē).</p>
System IDs	<p>Ļauj iestatīt:</p> <ul style="list-style-type: none"> Līdzekļu tagu (18 baitu identifikators) un īpašuma tagu (80 baitu identifikators, kas tiek parādīts POST darbības laikā). <p>Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Galddatora pārvaldības rokasgrāmata</i>.</p> <ul style="list-style-type: none"> Šasijas sērijas numuru un universālā unikālā identifikatora (UUID — Universal Unique Identifier) numuru. UUID var jaunināt tikai tad, ja pašreizējais šasijas sērijas numurs nav derīgs (parasti šie ID numuri tiek iestatīti rūpnīcā un lietoti, lai identificētu sistēmu). <p>Tastatūras lokalizācijas iestatījumi (piemēram, angļu vai vācu), lai ievadītu sistēmas ID.</p>
<p> Plašāku informāciju par utilītu Computer Setup skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Utilitās Computer Setup (F10) rokasgrāmata</i>.</p> <p>Drošības līdzekļu atbalsts var atšķirties atkarībā no konkrētās datora konfigurācijas.</p>	

Drošības līdzekļu pārskats (*turpinājums*)

Iespēja	Apraksts
DriveLock	<p>Ļauj piešķirt vai mainīt galveno vai lietotāja paroli MultiBay cietajiem diskkiem (netiek atbalstīta SCSI cietajiem diskkiem). Ja šis līdzeklis ir aktivizēts, POST darbības laikā lietotājam tiek piedāvāts ievadīt kādu no DriveLock parolēm. Ja nevienu paroli nevar veiksmīgi ievadīt, cietajam diskam nevarēs piekļūt līdz brīdim, kad kāda no parolēm tiks sekmīgi ievadīta nākošās aukstās sāknēšanas laikā.</p> <p> Šī iespēja tiek parādīta tikai tad, ja sistēmai ir pieslēgts vismaz viens MultiBay diskdzinis, kas atbalsta līdzekli DriveLock.</p> <p>Plašāku informāciju skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Galddatora pārvaldības rokasgrāmātā</i>.</p>
Master Boot Record Security	<p>Ļauj aktivizēt vai deaktivizēt līdzekli MBR Security.</p> <p>Ja tas ir aktivizēts, sistēma BIOS noraida visus rakstīšanas pieprasījumus pašreizējā sāknēšanas diska MBR. Ikreiz, kad dators tiek ieslēgts vai no jauna sāknēts, sistēma BIOS salīdzina pašreizējā sāknēšanas diska MBR ar iepriekš saglabāto MBR. Atrodot izmaiņas, tiek piedāvāts saglabāt pašreizējā sāknēšanas diska MBR, atjaunot iepriekš saglabāto MBR vai deaktivizēt līdzekli MBR Security. Ja ir iestatīta iestatījumu parole, tā ir jāzina.</p> <p> Pirms tišas pašreizējā sāknēšanas diska formatējuma vai nodalījumu maiņas deaktivizējiet līdzekli MBR Security. Vairākas diska utilītas (piemēram, FDISK un FORMAT) mēģina veikt MBR jaunināšanu.</p> <p>Ja ir aktivizēta līdzeklis MBR Security un piekļuvi diskam nodrošina sistēma BIOS, rakstīšanas pieprasījumi MBR tiek noraidīti un utilītas ziņo par kļūdām.</p> <p>Ja drošības līdzeklis MBR Security ir aktivizēts un piekļuvi diskam nodrošina operētājsistēma, nākamajā sāknēšanas reizē sistēma BIOS nosaka jebkādas MBR izmaiņas un tiek parādīts MBR Security brīdinājums.</p>
<p> Plašāku informāciju par utilītu Computer Setup skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Utilītas Computer Setup (F10) rokasgrāmātā</i>.</p> <p>Drošības līdzekļu atbalsts var atšķirties atkarībā no konkrētās datora konfigurācijas.</p>	

Drošības līdzekļu pārskats (turpinājums)

Iespēja	Apraksts
Save Master Boot Record	Saglabā pašreizējā sāknēšanas diska MBR dublējumkopiju. Tiek parādīta tikai tad, ja ir aktivizēts drošības līdzeklis MBR Security.
Restore Master Boot Record	<p>Atjauno MBR dublējumkopiju pašreizējā sāknēšanas diskā.</p> <p> Tiek parādīta tikai tad, ja ir iestatīti šādi parametri:</p> <ul style="list-style-type: none"> • ir aktivizēts līdzeklis MBR Security; • iepriekš ir saglabāta MBR dublējumkopija; • pašreizējais sāknēšanas disks ir tas pats disks, kuram tika saglabāta MBR dublējumkopija. <p> UZMANĪBU! Pēc iepriekš saglabāta MBR atjaunošanas, kad diska utilīta vai operētājsistēmas ir mainījusi MBR, diskā esošajiem datiem, iespējams, nevarēs piekļūt. Atjaunojiet iepriekš saglabātu MBR tikai tad, ja esat pārliecināts, ka pašreizējā sāknēšanas diska MBR ir bojāts vai inficēts ar vīrusu.</p>
<p> Plašāku informāciju par utilītu Computer Setup skatiet <i>dokumentācijas kompaktdiskā</i> iekļautajā <i>Utilītas Computer Setup (F10) rokasgrāmātā</i>.</p> <p>Drošības līdzekļu atbalsts var atšķirties atkarībā no konkrētās datora konfigurācijas.</p>	

Paroles drošība

Ieslēgšanas parole novērš nesankcionētu datora lietošanu, pieprasot ievadīt paroli, lai piekļūtu lietojumprogrammām vai datiem, ikreiz, kad dators tiek ieslēgts vai restartēts. Iestatījumu parole īpaši novērš nesankcionētu piekļuvi utilītai Computer Setup, un to var lietot arī ieslēgšanas paroles vietā. Kad tiek parādīts uzaicinājums ievadīt ieslēgšanas paroli, tās vietā var ievadīt iestatījumu paroli un piekļuve datoram tiek atļauta.

Var izveidot vispārēju tīkla paroli, kas sistēmas administratoram ļauj pieteikties visās tīkla sistēmās, lai veiktu apkopi, nezinot ieslēgšanas paroli, pat ja tā ir izveidota.

Iestatījumu paroles izveide, izmantojot utilītu Computer Setup

Ja sistēmā ir iegulta drošības ierīce, skatiet *dokumentācijas kompaktdiska* dokumentu *HP ProtectTools Embedded Security Guide*. Ja iestatījumu parole ir izveidota, izmantojot utilītu Computer Setup, nevar veikt datora rekonfigurāciju (Utilītas Computer Setup (F10) lietošana), līdz tiek ievadīta parole.

1. Ieslēdziet un restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators ir ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek palaista utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, datoru restartējot un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties **Security**, pēc tam izvēlieties **Setup Password** un izpildiet ekrānā redzamos norādījumus.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Ieslēgšanas paroles izveide, izmantojot utilītu Computer Setup

Ja ieslēgšanas parole ir izveidota, izmantojot utilītu Computer Setup, datoram nevar piekļūt, kad ir ieslēgta strāva, līdz tiek ievadīta parole. Ja ir iestatīta ieslēgšanas parole, utilītas Computer Setup izvēlnē Security ir pieejama iespēja Password Options. Paroles iespējas ietver Password Prompt on Warm Boot. Ja ir aktivizēta iespēja Password Prompt on Warm Boot, parole ir jāievada ikreiz, kad dators tiek atsāknēts.

1. Ieslēdziet un restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties **Security**, pēc tam **Power-on Password** un izpildiet ekrānā redzamos norādījumus.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Ieslēgšanas paroles ievadišana

Lai ievadītu ieslēgšanas paroli, veiciet šādas darbības:

1. Ieslēdziet un restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēšana) > Restart the Computer**.
2. Kad monitorā tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli un nospiediet taustiņu **Enter**.



Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

Ja parole ievadīta nepareizi, tiek parādīta salauztas atslēgas ikona. Mēģiniet vēlreiz. Pēc trīs neveiksmīgiem mēģinājumiem dators jāizslēdz un pēc tam no jauna jāieslēdz, lai turpinātu darbību.

Iestatījumu paroles ievadīšana

Ja sistēmā ir iegulta drošības ierīce, skatiet *dokumentācijas kompaktdiska* dokumentu *HP ProtectTools Embedded Security Guide*.

Ja datoram ir izveidota iestatījumu parole, ikreiz, palaižot utilītu Computer Setup, tiek lūgts ievadīt šo paroli.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Kad monitorā tiek parādīta atslēgas ikona, ievadiet iestatījumu paroli un nospiediet taustiņu **Enter**.



Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

Ja parole ievadīta nepareizi, tiek parādīta salauztas atslēgas ikona. Mēģiniet vēlreiz. Pēc trīs neveiksmīgiem mēģinājumiem dators jāizslēdz un pēc tam no jauna jāieslēdz, lai turpinātu darbu.

Ieslēgšanas vai iestatījumu paroles maiņa

Ja sistēmā ir iegulta drošības ierīce, skatiet *dokumentācijas kompaktdiska* dokumentu *HP ProtectTools Embedded Security Guide*.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart the Computer**.
2. Lai mainītu ieslēgšanas paroli, pārejiat uz 3. soli.

Lai mainītu iestatījumu paroli, tiklīdz dators tiek ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Kad tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli, slīpsvītru (/) vai citu norobežotāju, jauno paroli, vēl vienu slīpsvītru vai citu norobežotāju un vēlreiz — jauno paroli šādi: **pašreizējā parole/jaunā parole/jaunā parole**



Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

4. Nospiediet taustiņu **Enter**.

Jaunā parole stājas spēkā, kad nākamo reizi ieslēgsit datoru.



Plašāku informāciju par alternatīviem norobežotājiem skatiet „[Dažādām valodām paredzētie tastatūras norobežotāji](#)” lappusē 30. Ieslēgšanas paroli un iestatījumu paroli var mainīt arī, izmantojot utilītas Computer Setup iespēju Security (Drošība).

Ieslēgšanas vai iestatījumu paroles dzēšana

Ja sistēmā ir iegulta drošības ierīce, skatiet *dokumentācijas kompaktdiska* dokumentu *HP ProtectTools Embedded Security Guide*.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart the Computer**.
2. Lai izdzēstu ieslēgšanas paroli, pārejiet uz 3. soli.

Lai izdzēstu iestatījumu paroli, tiklīdz dators tiek ieslēgts, nospiediet un turiet taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apiētu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Kad tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli, pēc tam slīpsvītru vai citu norobežotāju šādi:
pašreizējā parole/
4. Nospiediet taustiņu **Enter**.



Plašāku informāciju par alternatīviem norobežotājiem skatiet [“Dažādām valodām paredzētie tastatūras norobežotāji”](#). Ieslēgšanas paroli un iestatījumu paroli var mainīt arī, izmantojot utilītas Computer Setup iespēju Security (Drošība).

Dažādām valodām paredzētie tastatūras norobežotāji

Katra tastatūra ir izstrādāta atbilstoši attiecīgās valsts prasībām. Sintakse un taustiņi, ko izmantojat, lai mainītu vai dzēstu paroli, ir atkarīgi no datora komplektācijā iekļautās tastatūras.

Dažādām valodām paredzēto tastatūru norobežotāji

Arābu	/	Itāliešu	-	Portugāļu	-
ASV angļu	/	Japāņu	/	Slovaku	-
Beļģu	=	Kanādas franču	é	Spāņu	-
BHCSY*	-	Korejiešu	/	Šveiciešu	-
Brazīliešu	/	Krievu	/	Taivaniešu	/
Čehu	-	Ķīniešu	/	Taju	/
Dāņu	-	Latīņamerikāņu	-	Turku	.
Ebreju	.	Lielbritānijas angļu	/	Ungāru	-
Franču	!	Norvēģu	-	Vācu	-
Grieķu	-	Poļu	-	Zviedru/somu	/

* Bosnija-Hercogovina, Horvātija, Slovēnija un Dienvidslāvija

Paroļu notīrīšana

Ja esat aizmirsis paroli, datoram piekļūt nav iespējams. Norādījumus par paroļu notīrīšanu skatiet *dokumentācijas kompaktdiskā* iekļautajā *Problēmu novēršanas rokasgrāmata*.

Ja sistēmā ir iegulta drošības ierīce, skatiet *dokumentācijas kompaktdiska* dokumentu *HP ProtectTools Embedded Security Guide*.

DriveLock

DriveLock ir nozares standartiem atbilstošs drošības līdzeklis, kas novērš nesankcionētu piekļuvi MultiBay cietajā diskā esošiem datiem. DriveLock ir izstrādāts kā utilītas Computer Setup paplašinājums. Tas ir pieejams tikai tad, ja dators ir atradis cietos diskus, kuriem var pievienot DriveLock.

Līdzeklis DriveLock ir piemērots tiem HP klientiem, kuri vislielāko vērību pievērš datu drošībai. Šiem klientiem cietā diska izmaksas un tajā glabāto datu zudums nav būtisks salīdzinājumā ar kaitējumu, kas var rasties nesankcionēti piekļūstot cietā diska saturam. Lai vienlaikus panāktu šāda līmeņa drošību un atrisinātu praktisku problēmu, ja aizmirsta parole, HP ir ieviesusi DriveLock divu paroļu drošības sistēmu. Vienu paroli iestata un lieto sistēmas administrators, bet otru parasti iestata un lieto galalietotājs. Ja abas paroles tiek pazaudētas, disku nav iespējams atbloķēt. Tāpēc DriveLock visdrošāk var lietot, ja cietajā diskā esošie dati tiek replicēti uzņēmuma informācijas sistēmā vai tiek regulāri veidotas to dublējumkopijas.

Ja abas DriveLock paroles tiek pazaudētas, cietais disks vairs nav lietojams. Lietotāji, kuru vajadzības atšķiras no iepriekš aprakstīto klientu vajadzībām, šādu risku, iespējams, neuzņemas. Lietotājiem, kas atbilst šo klientu aprakstam, šāds risks ir pieņemams, ņemot vērā cietajā diskā glabāto datu saturu.

DriveLock lietošana

Iespēja DriveLock tiek parādīta utilītas Computer Setup izvēlnē Security (Drošība). Lietotājam tiek piedāvāta iespēja iestatīt galveno paroli vai aktivizēt līdzekli DriveLock. Lai aktivizētu līdzekli DriveLock, ir jāievada lietotāja parole. Tā kā DriveLock sākotnējo konfigurāciju parasti veic sistēmas administrators, vispirms ir jāiestata galvenā parole. HP sistēmas administratoriem iesaka iestatīt galveno paroli neatkarīgi no tā, vai tie plāno aktivizēt līdzekli DriveLock. Tādējādi nākotnē administrators var mainīt DriveLock iestatījumus, ja disks ir bloķēts. Kad galvenā parole ir iestatīta, sistēmas administrators var aktivizēt līdzekli DriveLock vai arī atstāt to deaktivizētu.

Ja cietais disks ir bloķēts, POST pieprasa paroli, lai atbloķētu ierīci. Ja iestatītā ieslēgšanas parole sakrīt ar ierīces lietotāja paroli, POST neprasa lietotājam paroli ievadīt no jauna. Pretējā gadījumā lietotājam tiek pieprasīts ievadīt DriveLock paroli. Var lietot gan galveno gan lietotāja paroli. Lietotājs var divreiz mēģināt ievadīt pareizu paroli. Ja šie mēģinājumi neizdodas, POST turpina darbību, taču disks nav pieejams.

DriveLock lietojumprogrammas

Vispraktiskāk drošības līdzekli DriveLock var izmantot uzņēmuma vidē, kur sistēmas administrators lietotājiem nodrošina iespēju lietot MultiBay cietos diskus vairākos datoros. Sistēmas administrators ir atbildīgs par MultiBay cieto disku konfigurēšanu, kas cita starpā ietver DriveLock galvenās paroles iestatīšanu. Ja lietotājs aizmirst lietotāja paroli vai aprīkojums tiek nodots citam darbiniekam, galveno paroli vienmēr var izmantot, lai no jauna iestatītu lietotāja paroli un atjaunotu piekļuvi cietajam diskam.

HP ieteic uzņēmumu sistēmas administratoriem, kas vēlas aktivizēt līdzekli DriveLock, izstrādāt uzņēmuma politiku galveno parolu iestatīšanai un uzturēšanai. Šādi ir jārīkojas, lai nepieļautu situāciju, kad darbinieks pirms aiziešanas no uzņēmuma tīši vai netīši iestata abas DriveLock paroles. Tādā gadījumā cietais disks kļūst nederīgs un ir jānomaina. Ja galvenā parole nav iestatīta, var būt bloķēta sistēmas administratora piekļuve cietajam diskam un nevar veikt regulāras neautorizētas programmatūras pārbaudes, īstenot citu līdzekļu vadības funkcijas un atbalstu.


Lietotājiem, kuriem nav tik stingru drošības prasību, HP neiesaka aktivizēt līdzekli DriveLock. Tie ir personālo datoru lietotāji vai lietotāji, kas cietajā diskā nemēdz glabāt slepenus datus. Šiem lietotājiem cietā diska zaudējums, kas iespējams, ja aizmirstas abas paroles, ir daudz lielāks nekā DriveLock aizsargāto datu vērtība. Piekļuvi utilītai Computer Setup un līdzeklim DriveLock var ierobežot, izmantojot iestatījumu paroli. Nosakot iestatījumu paroli, kura netiek atklāta galalietotājiem, sistēmas administrators var nepieļaut līdzekļa DriveLock aktivizēšanu.

Sensors Smart Cover Sensor

Pārsega noņemšanas sensors (Cover Removal Sensor; pieejams atsevišķiem modeļiem) ir aparatūras un programmatūras tehnoloģiju kombinācija, kas brīdina, ja tiek noņemts datora pārsegs vai sānu panelis. Pastāv trīs līmeņu aizsardzība, kā redzams šajā tabulā.

Sensora Smart Cover Sensor aizsardzības līmeņi

Līmenis	Iestatījums	Apraksts
0 līmenis	Deaktivizēts	Sensors Smart Cover Sensor ir deaktivizēts (noklusējuma iestatījums).
1. līmenis	Notify User (Paziņot lietotājam)	Kad dators tiek restartēts, ekrānā tiek parādīts paziņojums par to, ka ir noņemts datora pārsegs vai sānu panelis.
2. līmenis	Setup Password (Iestatījumu parole)	Kad dators tiek restartēts, ekrānā tiek parādīts paziņojums par to, ka ir noņemts datora pārsegs vai sānu panelis. Lai turpinātu ir jāievada iestatījumu parole.

 Šos iestatījumus var mainīt, izmantojot utilītu Computer Setup. Plašāku informāciju par utilītu Computer Setup skatiet dokumentācijas kompaktdiskā iekļautajā *Utilītas Computer Setup (F10)* rokasgrāmātā.

Smart Cover Sensor drošības līmeņa iestatīšana

Lai iestatītu Smart Cover Sensor aizsardzības līmeni, izpildiet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apiētu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties **Security > Smart Cover > Cover Removal Sensor** un izvēlieties nepieciešamo drošības līmeni.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Slēdzene Smart Cover Lock

Slēdzene Smart Cover Lock ir ar programmartūru vadāma pārsega slēdzene, kas pieejama atsevišķiem HP datoriem. Šī slēdzene novērš nesankcionētu piekļuvi iekšējiem komponentiem. Iegādājoties datoru, slēdzene Smart Cover Lock ir atslēgtā stāvoklī.



UZMANĪBU! Lai nodrošinātu maksimālu pārsega slēdzenes drošību, izveidojiet iestatījumu paroli. Iestatījumu parole novērš nesankcionētu piekļuvi utilītai Computer Setup.



Slēdzene Smart Cover Lock ir iespēja, kas pieejama atsevišķiem modeļiem.

Slēdzenes Smart Cover Lock aizslēgšana

Lai aktivizētu un aizslēgtu slēdzeni Smart Cover Lock, veiciet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties iespēju **Security > Smart Cover > Cover Lock > Lock**.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Slēdzenes Smart Cover Lock atslēgšana

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet taustiņu **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties iespēju **Security > Smart Cover > Cover Lock > Unlock**.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Atslēgas Smart Cover FailSafe Key lietošana

Ja ir aktivizēta slēdzene Smart Cover Lock, taču nevar ievadīt paroli, lai slēdzeni deaktivizētu, datora pārsegu var atvērt, izmantojot atslēgu Smart Cover FailSafe Key. Atslēga ir nepieciešama šādos gadījumos:

- Strāvas pārtraukums
- Startēšanas kļūme
- Datora komponenta (piemēram, procesora vai barošanas bloka) kļūme
- Aizmirsta parole



UZMANĪBU! Atslēga Smart Cover FailSafe Key ir īpašs rīks, ko piedāvā HP. Lai nerastos neērtības, pasūtiet atslēgu pie pilnvarota izplatītāja vai pakalpojumu sniedzēja, pirms tā ir nepieciešama.

Lai iegādātos atslēgu FailSafe Key, veiciet kādu no šīm darbībām:

- Sazinieties ar pilnvarotu HP izplatītāju vai pakalpojumu sniedzēju.
- Zvaniet uz garantijā norādīto atbilstošo numuru.

Plašāku informāciju par atslēgas Smart Cover FailSafe Key lietošanu skatiet *dokumentācijas kompaktdiskā* iekļautajā *Aparatūras rokasgrāmatā*.

Master Boot Record Security

Galvenais sāknēšanas ieraksts (MBR — Master Boot Record) ietver informāciju, kas nepieciešama, lai veiksmīgi veiktu sāknēšanu no diska un lai piekļūtu diskā saglabātajiem datiem. Līdzeklis Master Boot Record Security nosaka un sniedz atskaiti par netīši vai ļaunprātīgi veiktām izmaiņām MBR, piemēram, datorvīrusa izraisītām izmaiņām vai izmaiņām, kas radušās diska utilītu nepareizas izmantošanas rezultātā. Tas ļauj arī atkopt „pēdējo labo” MBR, ja MBR izmaiņas ir noteiktas sistēmas restartēšanas laikā.

Lai aktivizētu līdzekli MBR Security, veiciet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties **Security > Master Boot Record Security > Enabled**.
4. Izvēlieties **Security > Save Master Boot Record**.
5. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Ja līdzeklis MBR Security ir aktivizēts, sistēma BIOS režīmā MS-DOS vai Windows drošajā režīmā neļauj veikt nekādas izmaiņas pašreizējā sāknēšanas diska MBR.



Lielākā daļa programmatūru vada piekļuvi pašreizējā sāknēšanas diska MBR, un sistēma BIOS nevar novērst izmaiņas, kas var rasties operētājsistēmas darbības laikā.

Ikreiz, kad dators tiek ieslēgts vai restartēts, sistēma BIOS salīdzina pašreizējā sāknēšanas diska MBR ar iepriekš saglabāto MBR. Ja tiek konstatētas izmaiņas un pašreizējais sāknēšanas disks ir tas pats disks, no kura iepriekš tika veikta MBR saglabāšana, tiek parādīts šāds paziņojums:

1999—Master Boot Record has changed.

Nospiediet jebkuru taustiņu, lai atvērtu programmu Setup un konfigurētu līdzekli MBR Security.

Pēc utilītas Computer Setup palaišanas:

- saglabājiēt pašreizējā sāknēšanas diska MBR;
- atjaunojiēt iepriekš saglabāto MBR vai
- deaktivizējiēt līdzekli MBR Security.

Ir jāzina iestatījumu parole, ja tāda ir norādīta.

Ja tiek konstatētas izmaiņas un pašreizējais sāknēšanas disks **nav** tas pats disks, no kura iepriekš tika veikta MBR saglabāšana, tiek parādīts šāds paziņojums:

2000—Master Boot Record Hard Drive has changed.

Nospiediet jebkuru taustiņu, lai atvērtu programmu Setup un konfigurētu līdzekli MBR Security.

Pēc utilītas Computer Setup palaišanas:

- saglabājiēt pašreizējā sāknēšanas diska MBR vai
- deaktivizējiēt līdzekli MBR Security.

Ir jāzina iestatījumu parole, ja tāda ir norādīta.

Ja iepriekš saglabātais MBR ir bojāts (maz iespējams), tiek parādīts šāds paziņojums:

1998—Master Boot Record has been lost.

Nospiediet jebkuru taustiņu, lai atvērtu programmu Setup un konfigurētu līdzekli MBR Security.

Pēc utilītas Computer Setup palaišanas:

- saglabājiēt pašreizējā sāknēšanas diska MBR vai
- deaktivizējiēt līdzekli MBR Security.

Ir jāzina iestatījumu parole, ja tāda ir norādīta.

Pirms pašreizējā sāknēšanas diska nodalīšanas vai formatēšanas

Pirms pašreizējā sāknēšanas diska nodalīšanas vai formatēšanas pārliecinieties, vai līdzeklis MBR Security ir deaktivizēts. Dažas diska utilītas, piemēram, FDISK un FORMAT, mēģina jaunināt MBR. Ja diska nodalīšanas un formatēšanas laikā ir aktivizēts līdzeklis MBR Security, diska utilīta var parādīt kļūdas paziņojumus vai, nākamreiz ieslēdzot vai restartējot datoru, līdzeklis MBR Security parāda brīdinājumu. Lai deaktivizētu līdzekli MBR Security, veiciet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start (Sākt) > Shut Down (Beidzēt) > Restart (Restartēšana)**.
2. Tiklīdz dators tiek ieslēgts, nospiediet un turiet nospiestu taustiņu **F10**, līdz tiek atvērta utilīta Computer Setup. Ja nepieciešams, nospiediet **Enter**, lai apietu nosaukuma ekrānu.



Ja taustiņš **F10** netiek nospiests īstajā brīdī, utilītai var piekļūt, restartējot datoru un vēlreiz nospiežot un turot taustiņu **F10**.

Lietojot PS/2 tastatūru, ekrānā tiek parādīts tastatūras kļūdas paziņojums Keyboard Error, ignorējiet to.

3. Izvēlieties **Security > Master Boot Record Security > Disabled**.
4. Pirms izešanas noklikšķiniet uz **File > Save Changes and Exit**.

Kabeļa slēdzenes nodrošinājums

Datora aizmugurējam panelim var uzstādīt kabeļa slēdzeni, lai dators fiziski tiktu nostiprināts pie darba virsmas.

Ilustrētus norādījumus skatiet *dokumentācijas kompaktdiskā* iekļautajā *Aparatūras rokasgrāmata*.

Pirkstu nospiedumu identificēšanas tehnoloģija

Lai nebūtu jāievada lietotāju paroles, HP tehnoloģija Fingerprint Identification paaugstina tīkla drošību, vienkāršo pieteikšanās procesu un samazina ar kopējo tīklu pārvaldību saistītās izmaksas. Par pašreizējo cenu šo tehnoloģiju var atļauties iegādāties ne tikai progresīvo tehnoloģiju un augstas drošības organizācijās.



Pirkstu nospiedumu identificēšanas tehnoloģijas atbalsts ir atkarīgs no datora modeļa.

Lai iegūtu plašāku informāciju, apmeklējiet:

<http://h18004.www1.hp.com/products/security/>.

Kļūdu paziņojumi un atkopšana

Līdzekļi Fault Notification un Recovery apvieno jaunas aparatūru un programmatūras tehnoloģijas, kas novērš svarīgu datu zaudēšanu un samazina neplānotas dīkstāves risku.

Ja dators ir pieslēgts tīklam, ko pārvalda programmatūra HP Client Manager, dators nosūta kļūdas paziņojumu tīkla pārvaldības lietojumprogrammai. Izmantojot programmatūru HP Client Manager, var attāli plānot diagnostiku, lai to automātiski palaistu uz visiem pārvaldītajiem datoriem un izveidotu kopsavilkuma atskati par neapmierinošajiem pārbažu rezultātiem.

Disku aizsardzības sistēma

Drive Protection System (DPS) ir cietajā diskā iebūvēts diagnostikas rīks, kas uzstādīts atsevišķiem HP datoriem. DPS ir izstrādāts, lai diagnosticētu problēmas, kas var rasties patvaļīgas cietā diska nomaiņas rezultātā.

Montējot HP datorus, katrs uzstādītais cietais disks tiek pārbaudīts, izmantojot DPS, un šajā diskā tiek izveidots pamatinformācijas pastāvīgais ieraksts. Ikreiz, kad tiek palaists rīks DPS, pārbaudes rezultāti tiek ierakstīti cietajā diskā. Pakalpojumu sniedzējs var izmantot šo informāciju, lai diagnosticētu apstākļus, kuros tika palaista DBS programmatūra. Norādījumus par DPS lietošanu skatiet *dokumentācijas kompaktdiskā* iekļautajā *Problēmu novēršanas rokasgrāmātā*.

Izlīdzinošs barošanas bloks

Iebūvēts izlīdzinošais barošanas bloks sniedz drošību, ja notiek neparedzēta strāvas pārslodze. Šis barošanas bloks var izturēt ne vairāk kā 2000 voltu strāvas pārslodzi, neradot sistēmas dīkstāvi vai datu zudumu.

Termiskais sensors

Termiskais sensors ir aparātūras un programmatūras līdzeklis, kas kontrolē datora iekšējo temperatūru. Šis līdzeklis parāda brīdinājuma paziņojumu, ja tiek pārsniegts noteiktais temperatūras diapazons; tas ļauj veikt aizsardzības pasākumus, pirms tiek bojāti datora iekšējie komponenti vai zaudēti dati.

Alfabētiskais rādītājs

A

Altiris 4
atkopšana, programmatūra 2
Attāla sistēmas instalēšana, piekļuve 3
attāla uzstādīšana 3

B

barošanas bloks, izlīdzinošs 40
brīdinājumi
 FailSafe Key 35
 pārsega slēdzenes drošība 34
 ROM aizsardzība 7

C

cietā diska aizsardzība 39
cietā diska diagnostikas rīks 39
cietie diski, diagnostikas rīks 39

D

datora iekšējā temperatūra 40
datora piekļuves vadīšana 20
datu izsekošana 20
dažādām valodām paredzēto tastatūru
 norobežotāji 30
diska formatēšana, svarīga informācija 38
diska nodalīšana, svarīga informācija 38
DiskOnKey
 sk. arī HP Drive Key
 sāknēšanas 13 - 18
disks, aizsardzība 39
disks, klonēšana 2
divstāvokļu strāvas poga 18

Drivelock 31 - 32

drošība

 DriveLock 31 - 32
 iestatījumi, iestatīšana 20
 līdzekļi, tabula 21
 Master Boot Record 36 - 37
 MultiBay 31 - 32
 parole 24
 Smart Cover Lock 34 - 35
 Smart Cover Sensor 32

F

FailSafe Key
 brīdinājums 35
 pasūtīšana 35
FailSafe Key pasūtīšana 35
FailSafe sāknēšanas bloka ROM 8

H

HP Client Manager 4
HP Drive Key
 sk. arī DiskOnKey
 sāknēšanas 13 - 18

I

ieslēgšanas parole
 dzēšana 29
 ievadīšana 26
 mainīšana 28
iestatījumi
 sākotnējie 2

iestatījumu parole

dzēšana 29

iestatījumi 25

ievadīšana 27

mainīšana 28

iestatīšana

replicēšana 10

ievadīšana

ieslēgšanas parole 26

iestatījumu parole 27

ieviešanas rīki, programmatūra 2

Interneta adreses, Sk. Web vietas

izlīdzinošs barošanas bloks 40

izmaiņu paziņošana 6

K

kabeļa slēdzenes nodrošinājums 38

klonēšanas rīki, programmatūra 2

kļūdu paziņojumi 39

L

lasāmatmiņas aizsardzība, brīdinājums 7

M

Master Boot Record Security 36 - 37

Multibay drošība 31 - 32

N

nederīga sistēmas ROM 8

norobežotāji, tabula 30

O

operētājsistēmas mainīšana, svarīga

informācija 19

operētājsistēmas, svarīga informācija par 19

P

PXE (Preboot Execution Environment) 3

parole

drošība 24

dzēšana 29

ieslēgšana 26

iestatīšana 25, 27

mainīšana 28

notīrīšana 30

paroles dzēšana 29

paroles mainīšana 28

paroļu notīrīšana 30

paziņošana par izmaiņām 6

pārsega slēdzene, viedā 34

pārsega slēdzenes drošība, brīdinājums 34

PCN (Proactive Change Notification) 6

piekļuve datoram, kontrolēšana 20

pirkstu nospiedumu identificēšanas

tehnoloģija 39

Preboot Execution Environment (PXE) 3

Proactive Change Notification (PCN) 6

programmatūra

atkopšana 2

datu izsekošana 20

Drive Protection System 39

FailSafe sāknēšanas bloka ROM 8

Fault Notification un Recovery 39

integrēšana 2

Master Boot Record Security 36 - 37

Remote ROM Flash 7

Remote System Installation 3

System Software Manager 6

utilīta Computer Setup 10

vairāku datoru jaunināšana 6

programmatūras pielāgošana 2

R

ROM

- Attāla pārrakstīšana 7
- jaunināšana 7
- nederīga 8
- tastatūras indikatori, tabula 9

ROM jaunināšana 7

S

- sāknēšanas disks, svarīga informācija 38
- sāknēšanas ierīce
 - DiskOnKey 13 - 18
 - HP Drive Key 13 - 18
 - izveide 13 - 18
 - USB zibatmiņas datu nesējs 13 - 18
- sākotnējā konfigurācija 2
- sākotnēji instalēts programmatūras attēls 2
- Sensors Smart Cover Sensor
 - iestatīšana 33
- sistēmas atkopšana 8
- Smart Cover FailSafe Key, pasūtīšana 35
- Smart Cover Lock 34 - 35
 - aizslēgšana 34
 - atslēgšana 35
- Smart Cover Lock aizslēgšana 34
- Smart Cover Lock atslēgšana 35
- Smart Cover Sensor 32
 - aizsardzības līmeņi 33
- SSM (System Software Manager) 6
- strāvas poga
 - divstāvokļu 18
 - konfigurēšana 18
- strāvas pogas konfigurēšana 18
- System Software Manager (SSM) 6

T

- tastatūras indikatori, ROM, tabula 9
- tastatūras norobežotāji, nacionālie 30
- temperatūra, datora iekšējie komponenti 40
- termiskais sensors 40

U

- URL (Web vietas). Sk. Web vietas
- USB zibatmiņas datu nesējs,
 - sāknēšanas 13 - 18
- Utilīta Computer Setup 10

W

- Web vietas
 - Altiris 5
 - Fingerprint Identification Technology 39
 - HP Client Manager 4
 - HPQFlash 8
 - iestatījumu replicēšana 12, 13
 - PC deployment 2
 - Proactive Change Notification 6
 - programmatūras atbalsts 19
 - Remote ROM Flash 7
 - ROM Flash 7
 - ROMPaq images 7
 - Subscriber's Choice 6
 - System Software Manager (SSM) 6